UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	**CRIMINAL ACTION**
v.	)	**NO. 4:19-40044-TSH**
KENNETH GIANATASIO,	)	
Defendant.	)	

MEMORANDUM AND ORDER ON DEFENDANT'S MOTION TO SUPPRESS EVIDENCE (Docket No. 53)

December 17, 2021

HILLMAN, D.J.

The United States of America charged the defendant, Kenneth Gianatasio, with distribution and possession of child pornography. The distribution charge is based on an image the defendant allegedly distributed over an instant messaging application. The Canadian company that operated the application used automated software to detect the image. Subsequently, the company generated a report and sent the report and image to Canadian law enforcement. Canadian law enforcement then forwarded the materials to law enforcement in the United States. Without a warrant, a law enforcement officer in the United States viewed the image.

The defendant moves to suppress the image, asserting that the officer's examination of the image without a warrant was an unreasonable search under the Fourth Amendment. Because an employee of the company viewed the image prior to sending it to law enforcement, or, even if not, because the officer who viewed the image reasonably relied on the company's representation that one did, the Court ***denies*** the defendant's motion.

Background

In September 2019, law enforcement officers in the United States came to suspect that the defendant had distributed an image of child pornography on Kik Messenger, an instant messaging application for mobile devices. At the time, a Canada-based technology company called Kik Interactive, Inc. ("Kik") operated Kik Messenger. Kik used a technology called PhotoDNA, developed by Microsoft, to detect images of child pornography uploaded to Kik Messenger. PhotoDNA used a kind of "hashing" to create a unique signature for each digital image it scanned. To detect images of child pornography, PhotoDNA cross-referenced images uploaded to Kik Messenger with a database of images previously identified as child pornography.[1]

Yves Savard, who led Kik's content moderation and law enforcement response teams in August and September of 2019, testified regarding Kik's procedures for identifying illegal images and sending those images to law enforcement. When PhotoDNA detected a match between an image uploaded to Kik Messenger and an image in Kik's database, Kik would suspend the account that uploaded the image and place the image into an electronic "review bucket." PhotoDNA flagged anywhere from 10 to 500 images per day. Because not all flagged images were illegal under Canadian law, however, a Kik employee would review each flagged image to determine whether the image in fact was illegal.[2] Only after an employee confirmed that the image was illegal would Kik terminate the account that uploaded the image and generate a report to send it to law enforcement. Indeed, Savard testified that an image flagged by PhotoDNA could not be sent

[1] To ensure that at least 95% of images in its database were illegal under Canadian law, Kik reviewed random samples of images before accepting batches of images into its database.

[2] Recall that the accuracy threshold for accepting an image into Kik's database was 95%.

to law enforcement without an employee reviewing the image first. Although the initial flag of an image by PhotoDNA was automated, the review and reporting process thereafter was manual.[3]

Here, Special Agent Edward Bradsheet contacted Canadian law enforcement to determine whether Kik had reported any information concerning the defendant's Kik Messenger account. Subsequently, Canadian law enforcement sent Agent Bradsheet materials received from Kik. The materials included an image, a report, and a glossary describing Kik's procedures. The procedures, which Agent Bradsheet reviewed prior to viewing the image and with which Agent Bradsheet was familiar due to his prior experience with Kik, stated that a Kik employee reviewed each image identified by PhotoDNA prior to reporting the image to law enforcement. The report indicated that PhotoDNA had detected the image at issue here on August 6, 2019.

While certain information concerning the manual review of images flagged by PhotoDNA -- such as the identity of the employee who confirmed that the image contained child pornography -- was not sent to law enforcement, Savard testified that it would have been possible, at least at the time, for Kik to determine which employee had reviewed each image. Kik, however, sold Kik Messenger to an American company in October 2019, and the American company does not keep such records. Nonetheless, based on Kik's standard procedures and Savard's testimony, the Court finds that a Kik employee viewed the image at issue here prior to sending it to Canadian law

[3] After PhotoDNA flagged an image and placed it into the electronic review bucket, an employee, at his or her computer, would click on the bucket, prompting the flagged images to pop up on his or her screen one-by-one. If the employee deemed the image to be illegal under Canadian law, the employee would click "yes." When the employee clicked "yes," the image would be sent to another bucket from which a report would be generated. To generate the report, the employee would click on the account name in that second bucket, which would download the image and various other data. Each day, an employee would package the generated reports into an electronic folder, look through the folder to make sure no files were corrupted, and then send the folder to law enforcement.

enforcement. Indeed, nothing in the record suggests that Kik did not follow its standard procedures in this case.

Discussion

1. Private Search Doctrine

The parties appear to agree that Agent Bradsheet's examination of the image was a search. The Court, therefore, will assume that the defendant had a reasonable expectation of privacy in the image. *See United States v. Powell*, 925 F.3d 1, 5 (1st Cir. 2018); *see also United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010).

The Fourth Amendment protects against governmental intrusion. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984). When a private actor invades a person's reasonable expectation of privacy, there is no Fourth Amendment violation. *See United States v. Rivera-Morales*, 961 F.3d 1, 8 (1st Cir. 2020). Under the private search doctrine, there likewise is no Fourth Amendment violation when the government conducts a search that is "coextensive with the scope of the private actor's private search and there is 'a virtual certainty that nothing else of significance' could be revealed by the governmental search." *Powell*, 925 F.3d at 5 (quoting *Jacobsen*, 466 U.S. at 119).

In *Powell*, 925 F.3d at 3, the First Circuit considered a defendant's request to withdraw a guilty plea based on his counsel's failure to move to suppress screenshots of suspected child pornography that a private company had sent to law enforcement. The company, which operated a video chat service that automatically and periodically took screenshots of its users' chats, sent screenshots to law enforcement after reviewing the screenshots and confirming that they contained child pornography. *Id.* at 3-4. The court denied the defendant's motion to withdraw his guilty plea, reasoning that the defendant had failed to show a Fourth Amendment violation because the

images reviewed by law enforcement were "precisely the ones that had already been viewed by the private actor." *Id.* at 6.

The same reasoning applies here. After automated software flagged the image uploaded by the defendant, a Kik employee reviewed the image to confirm that it contained child pornography. Kik then sent the image to Canadian law enforcement, which later forwarded it to United States law enforcement. When Agent Bradsheet ultimately viewed the image, he did no more than replicate Kik's private search. Because a Kik employee had viewed the image to confirm that it was child pornography, there was a "virtual certainty" that the search would reveal nothing more to Agent Bradsheet than it did to Kik. *See Jacobsen*, 466 U.S. at 119.

The cases relied on the by the defendant are distinguishable. In *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016), the government viewed more than what the company's automated software had detected as child pornography. Here, Agent Bradsheet viewed only the image flagged by PhotoDNA. In *United States v. Keith*, 980 F. Supp. 2d 33, 37 (D. Mass. 2013), and *United States v. Wilson*, 13 F.4th 961, 964 (9th Cir. 2021), no employee viewed the suspect image prior to sending it to law enforcement. Indeed, in *Wilson*, 13 F.4th at 974, the "critical fact" was that no "employee viewed [the defendant's] files before [the officer] did." Here, as stated, a Kik employee reviewed the image prior to sending it to law enforcement. Accordingly, the defendant's Fourth Amendment rights were not violated, and suppression of the image is not warranted.

2. Good Faith Exception

Even if, in this case, a Kik employee did not view the image prior to sending it to law enforcement, the good faith exception to the exclusionary rule would apply. "The exclusionary rule operates as a judicially created remedy designed to safeguard against future violations of

Fourth Amendment rights through the rule's general deterrent effect." *Arizona v. Evans*, 514 U.S. 1, 10 (1995). "Police practices trigger the harsh sanction of exclusion only when they are deliberate enough to yield 'meaningfu[l]' deterrence, and culpable enough to be 'worth the price paid by the justice system.'" *Davis v. United States*, 564 U.S. 229, 240 (2011) (quoting *Herring v. United States*, 555 U.S. 135, 144 (2009)). Here, Kik's standard procedure was for employees to review each image flagged by PhotoDNA before sending the image to law enforcement. This procedure was expressly stated in the glossary that was forwarded, along with the image, to Agent Bradsheet. Agent Bradsheet credibly testified that he was aware of the procedure -- from having frequently received leads from Kik, from having read guidance concerning PhotoDNA from the Department of Justice, and from having reviewed Kik's glossary before viewing the image. Because Agent Bradsheet reasonably relied on Kik's representation, *see United States v. Bonds*, 2021 WL 4782270, at *5 (W.D.N.C. Oct. 13, 2021), suppression of the image would serve no meaningful deterrent effect.

Conclusion

For the reasons stated above, the Court ***denies*** the defendant's motion to suppress.

SO ORDERED

/s/ Timothy S. Hillman
TIMOTHY S. HILLMAN
DISTRICT JUDGE